



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/518,782	03/03/2000	Kouya Tochikubo	04329.22444	7469
22852	7590	02/28/2005		EXAMINER
FINNNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			BROWN, CHRISTOPHER J	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 02/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.	09/518,782	Applicant(s)	TOCHIKUBO ET AL.
Examiner	Christopher J Brown	Art Unit	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

1) Responsive to communication(s) filed on 16 December 2004.  
2a) This action is **FINAL**.                            2b) This action is non-final.  
3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

4) Claim(s) 4,5,7-13 and 17-25 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) Claim(s) 4,5,7,13,17-19 and 22-24 is/are allowed.  
6) Claim(s) 8-12,20,21,25 is/are rejected.  
7) Claim(s) \_\_\_\_\_ is/are objected to.  
8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

9) The specification is objected to by the Examiner.  
10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) All    b) Some \* c) None of:  
1. Certified copies of the priority documents have been received.  
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

1) Notice of References Cited (PTO-892)  
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) Notice of Informal Patent Application (PTO-152)  
6) Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

1. Applicant's arguments, see with respect to the rejection(s) of claim(s) 22 and 23 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of 112 issues and new claim 25.

### ***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 8 recites the limitation "the partner" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation "the partner" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 20 recites the limitation "cryptographic communication center apparatus" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claims 10, 11, 12, and 21 are rejected as being dependent on the above rejected claims

Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular the last paragraph, if the examiner is interpreting it correctly, does not match the instant specification and is hard to follow in general. The last paragraph seems to indicate (line 1) encrypting “the cryptographic algorithm” using (line 3) “the cryptographic algorithm” In essence the “encryption/decryption” section uses an algorithm to encrypt itself.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 5,199,069, Barrett et al. in view of US 2000/0046564, Masuda et al. and in further view of US 6,249,866 Brundrett et al. and in further view of US 6,694,025, Epstein et al.

Regarding claim 25, Barrett shows a cryptographic communication terminal comprising:

A cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication (Barrett, col. 3, line 58-60), outputting a designated cryptographic algorithm, said cryptographic algorithm storage section storing an encrypted cryptographic algorithm (synchronization, Barrett, col. 4, line 14-16, 29-31); control means for designating, with respect to said cryptographic algorithm storage section and said key information storage section, which cryptographic algorithm and key are to be used in the cryptographic communication (Barrett, col. 2, line 15-17; col. 3, line 54-56); and encryption/decryption means for decrypting received encryption information by using the cryptographic algorithm designated with respect to said cryptographic algorithm storage section and the key designated with respect to said key information storage section, and encrypting information to be transmitted (Barrett col. 4, line 60-624 col. 5, line 2 1-23) but fail to show:

- (a) a cryptographic algorithm decryption means of decrypting the encrypted cryptographic algorithm;
- (b) key information decryption means for decrypting an encrypted key from said key information storage section; a key information storage section for storing a key used for cryptographic communication corresponding to the cryptographic algorithm, and outputting a designated key, said key information storage section storing a key for an encrypted algorithm used to decrypt an encrypted cryptographic algorithm
- (c) as well as the key for cryptographic communication;

however,

- a) Masuda shows a system where a medium for storing (algorithm storage section) an algorithm encrypted together with the data. A loader in the device driver 22 loads the encrypted algorithm 34 into the PC (terminal) 11, transmits it to the server 33 (decrypting means), and requested the server 33 to decrypt the algorithm 34. Then the loader 31 receives the algorithm decrypted by the server 33 and transmits it to the decrypting unit 23. The decrypting unit 23 decrypts the data according to transmitted algorithm (Masuda, fig. 6, pp. 2, para. 0046).
- b) Brundrett teaches an encryption key that is a random number encrypted by the public key of at least one user and at least one recovery agent. These keys are stored with the files (key information storage section), whereby the file can always be decrypted by the private key of either a user or a recovery agent (Brundrett, col. 2, line 41-44, col. 10, line 13-15).
- c) Epstein teaches network system where the server contains a list of public/private key pairs, wherein the private key is stored in an encrypted form (Epstein, col. 3, line 63-65). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Masuda and Brundrett and Epstein to include encrypted decryption algorithm such that Barrett gains the advantage of further improving the security for the data stored on the storage medium (Masuda, pp. 1, para. 0017) and provide a strong cryptographic solution that addresses encryption data recovery (Brundrett, col. 2, line 21-22) and to provide a method for securely storing private keys in a networked environment (Epstein, col. 2, line 53-55).

***Allowable Subject Matter***

4. Claims 22, 23 and their dependant claims would be considered allowable if the previous 112 rejections in this action were overcome.

***Conclusion***

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J. Brown

02/17/05



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100